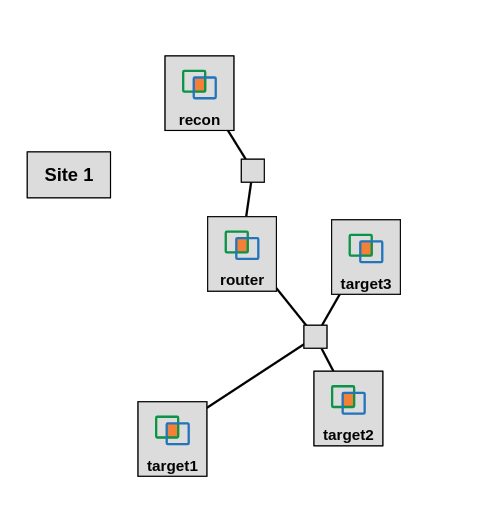
**CTF Challenge: Network Reconnaissance**

****

**Goals of Reconnaissance:**

****

* **Identify Vulnerabilities:** By understanding the target's systems, software, and configurations, attackers (or security professionals) can pinpoint potential weaknesses to exploit.
* **Plan the Attack (or Defense):** The information gathered allows for planning a targeted attack strategy or designing effective security measures to defend against potential threats.
* **Minimize Risk:** By understanding the target's defenses, attackers can minimize the risk of detection during their operations. Security professionals can use this knowledge to strengthen their own defenses.

**Techniques of Reconnaissance:**

****

**Footprinting:** Gathering basic info like IP address, domain name, and network range. (Imagine following someone's footprints)

**Enumeration:** Identifying services, applications, and user accounts running on the target. (Like making a list of everything in their house)

**Port Scanning:** Probing ports to see which ones are open and what services are running on those ports. (Checking which doors and windows are open)

**Web Application Scanning:** Analyzing a website for vulnerabilities specific to web applications. (Looking for weak points in the house's security system)

**Wireless Network Scanning:** Discovering available wireless networks and potential vulnerabilities. (Identifying unlocked cars in the driveway)

**Ethical Considerations:**

It's crucial to conduct reconnaissance ethically and legally. Security professionals typically perform reconnaissance with authorization and within the legal boundaries. Attackers, on the other hand, engage in reconnaissance for malicious purposes, which is illegal.

# **Capture the Flag (CTF) Challenges**

Flag 1. What information gathering technique focuses on collecting basic details like IP address and domain name?

Answer: Footprinting

Flag Captured

Flag 2. Which reconnaissance technique involves identifying services running on specific ports?

Answer: Port Scanning

Flag Captured

Flag 3. How can ethical reconnaissance help security professionals improve defenses? Answer: Planning

Flag Captured

Flag 4. Typically conducts reconnaissance without authorization and for malicious purposes?

Answer: Attackers

Flag Captured